



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/822,548	03/30/2001	Matthew D. Wood	42390P10451	7654
7590	10/11/2006			EXAMINER PYZOWCHA, MICHAEL J
Michael A. DeSanctis BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP Seventh Floor 12400 Wilshire Boulevard Los Angeles, CA 90025-1026			ART UNIT 2137	PAPER NUMBER

DATE MAILED: 10/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/822,548	WOOD ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 28 August 2006.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-3,5-9,17-20,25-27,29 and 30 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-3,5-9,17-20,25-27,29 and 30 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____

5) Notice of Informal Patent Application

6) Other: _____

DETAILED ACTION

1. Claims 1-3, 5-9, 17-20, 25-27, and 29-30 are pending.
2. Response filed 08/28/2006 has been received and fully considered. Applicant stated claims 1-3, 5-9, 17-20, 25-27, and 39-30 are pending but this was clearly a typo as claims 1-3, 5-9, 17-20, 25-27, and 29-30 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5-9, 17-20, 25-27, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Jr. et al (US 6687375), in view of Chen et al (US 6182220), further in view of Hardy et al (US 6073242), and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 1, 17 and 25, Matyas Jr. et al discloses initializing a pseudo-random number generator (PRNG); obtaining

local seeding information from a host; obtaining additional seeding information from one or more sources; and stirring the PRNG with the local seeding information and the additional seeding information (see column 9 lines 19-34 and 45-67).

Matyas Jr. et al fails to disclose securely obtaining additional seeding information from one or more remote entropy servers.

However, Chen et al teaches obtaining seeding information from one or more remote entropy servers (see column 1 line 66 through column 2 line 9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to obtain the additional seeding information of Matyas Jr. et al from the server of Chen et al.

Motivation to do so would have been to update passwords on the server (see Chen et al column 4 lines 15-39).

The modified Matyas Jr. et al and Chen et al system fails to disclose the communication between host and server being secure.

However, Hardy et al teaches secure communications (see column 3 lines 54-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Hardy et al's

method of secure communications in the modified system of Matyas Jr. et al and Chen et al system.

Motivation to do so would have been to provide confidentiality, authentication and integrity to the communications (see column 3 lines 54-67).

The modified Matyas Jr. et al, Chen et al, and Hardy et al system fails to disclose the specific method of securely obtaining the keys, data and obtaining seeding information from each location.

However, Menezes et al teaches the key exchanging (see section 12.5.1), the use of temporary keys (see page 494), the use of a public key encryption scheme (see section 1.8.1) and obtaining a large amount of seeding information (see pages 170-171).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the methods of Menezes et al to securely obtain the seeding information of the modified Matyas Jr. et al, Chen et al, and Hardy et al system.

Motivation to do so would have been to transport the key (see section 12.5.1), to limit the available ciphertext (see page 494), only the private key must be kept secret (see section 1.8.4) and seeds should be sufficiently large so that a search of all seeds is infeasible (see page 171).

As per claims 2-3 and 26-27, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the initializing the PRNG comprises initializing the internal state of the PRNG with a random value that is a seed (see Matyas Jr. et al column 9 lines 19-34).

As per claims 5 and 29, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the one or more remote entropy servers maintain random state pool to supply the host with the random value (see Matyas Jr. et al column 9 lines 45-67).

As per claim 6-8, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the securely obtaining seeding information from the one or more remote entropy servers may include using a privacy protocol, wherein the privacy protocol comprises secure sockets layer (SSL) protocol and transport layer security (TLS) protocol (see Hardy et al column 3 lines 54-67).

As per claims 9 and 30, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the stirring the PRNG comprises producing a cryptographically random stream of bits (see Matyas Jr. et al column 9 lines 45-67).

As per claim 18, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the local system

Art Unit: 2137

generates local seeding information (see Matyas Jr. et al column 9 lines 45-67).

As per claim 19, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system discloses the one or more remote systems generate remote seeding information (see Chen et al column 1 line 66 through column 2 line 9).

As per claim 20, the modified Matyas Jr. et al, Chen et al, Hardy et al, and Menezes et al system the entropy servers are hardware or software (see Chen et al column 4 lines 40-54).

Response to Arguments

5. Applicant's arguments filed 08/28/2006 have been fully considered but they are not persuasive. Applicant argues Chen fails to disclose "securely obtaining additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of additional seeding information is repeated for each entropy server".

With respect to Applicant's argument that Chen fails to disclose "securely obtaining additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of additional seeding information is repeated for each entropy

server", Chen is not relied upon to teach every element listed. Chen is relied upon for the teaching of obtaining random seeding information from one or more remote entropy servers, as applied to the multiple seeds of Matyas Jr. et al the combined system teaches obtaining additional seeding information from one or more remote entropy servers. Furthermore, this modified system fails to disclose the obtaining is done over a secure communication; this limitation is met by the Hardy system as put forth above. The repetition for each entropy server is taught by Menezes as discussed above. Finally, the combination of all the references teaches the secure entropy collection protocol as defined in the claim language. Applicant is reminded that the combined references must be considered as a whole. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS

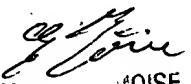
of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER